Privacy Impact Assessment (PIA): CDC - Lucid - QTR1 - 2024 - CDC7762606

Created Date: 12/31/2024 11:00 AM Last Updated: 2/20/2025 3:01 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	CDC - Lucid - QTR1 - 2024 - CDC7762606	**PIA ID:**	2596934
Name of Component:	CDC - Lucid Govsuite	**Name of ATO Boundary:**	Lucid Govsuite
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	386
Submission Status:	Re-Submitted	**Submit Date:**	1/23/2025
Next Assessment Date:	N/A	**Expiration Date:**	2/20/2028
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC7762606
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Development
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	The purpose of Lucid Govsuite, which includes Lucidchart and Lucidspark, is to provide a collaborative platform for creating diagrams and brainstorming. The system is a product of Lucid Software, Inc. The product is used by Centers for Disease Control and Prevention (CDC)/Office of the Chief Operating Officer (OCOO)/Office of the Chief Information Officer (OCIO)/Digital Services Office (DSO). Engineers and Product Owners use Lucid Govsuite to create visual content, collaborate on projects, and facilitate virtual brainstorming sessions. Users who create and collaborate on documents own the data within the system. Users within organizations and teams use data for content creation, collaboration, and visualization purposes to enhance their projects. Engineers and Product Owners can export the diagrams, chart, and text as png files and attached to O365 Sharepoint or O365 Teams.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	This system collects various types of data, including diagrams, charts, text, and user metadata. Lucid collects data on user interactions with the platform to improve their platform. Lucid can be used in a way for researchers or product owners to conduct usability interviews as research topics for user interfaces. These interviews could include the interviewee's name inadvertently as part of the documentation stored in Lucid. We intend to limit it as administrators but would like to be able to cover this 1% use case. While it is possible for PII data to be in Lucid, this is a extremely small percentage use case. The major use case of this service is to support engineers and product owners to draw out their thoughts collaboratively, which includes no PII at all. The Lucid application gathers and track first name, last name, and email of the user of the application for follow up purposes.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	This system collects various types of data, including diagrams, charts, text, and user metadata. Lucid collects data on user interactions with the platform to improve their platform. Lucid can be used in a way for researchers or product owners to conduct usability interviews as research topics for user interfaces. These interviews could include the interviewee's name inadvertently as part of the documentation stored in Lucid. We intend to limit it as administrators but would like to be able to cover this 1% use case. While it is possible for PII data to be in Lucid, this is a extremely small percentage use case. The major use case of this service is to support engineers and product owners to draw out their thoughts collaboratively, which includes no PII at all. The Lucid application gathers and track first name, last name, and email of the user of the application for follow up purposes.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The purpose of Lucid Govsuite, which includes Lucidchart and Lucidspark, is to provide a collaborative platform for creating diagrams and brainstorming. The system is a product of Lucid Software, Inc. The product is used by Centers for Disease Control and Prevention (CDC)/Office of the Chief Operating Officer (OCOO)/Office of the Chief Information Officer (OCIO)/Digital Services Office (DSO). Engineers and Product Owners use Lucid Govsuite to create visual content, collaborate on projects, and facilitate virtual brainstorming sessions. Users who create and collaborate on documents own the data within the system. This system collects various types of data, including diagrams, charts, text, and user metadata. Lucid collects data on user interactions with the platform to improve their platform.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
PTA - 12:	Does the website use web measurement and customization technology?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Collect PII Session Cookies - Does Not Collect PII

PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	Third-party
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	TBD
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	Yes
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	Yes
PTA - 18:	Does the mobile application use measurement and customization technology?	Yes
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	Lucid Govsuite tracks users requests to track utilization of the software in order for Lucid admins to determine utilization of the software. These utilizations are tracked via standard HTTP requests going to Lucid Govsuite. Lucid is GPDR compliant and will delete collected user information (username and email) if CDC decides to delete the account as per https://lucid.co/gdpr-compliance/.
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	Yes
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	No
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	No
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Mailing Address
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000

PIA - 4:	For what primary purpose is the PII used?	The primary purpose for name and email address is for access to Lucid Govsuite. The uses of phone numbers and mailing addresses incidentally displayed in the context of whiteboard documentation is as varied as the functions and activities of Lucid users. Users may document their contact information in order to be reached about a particular document or project.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no intended secondary uses for which the PII will be used.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable - SSNs are not used in the operation of this system.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable - SSNs are not used in the operation of this system.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. 301 which provides authority for the agency to establish the organizations, procedures and tools necessary to perform its duties and pursue its mission. Information use and disclosure for this system is governed by the laws and regulations of the individual business practice that this system is used to conduct. Users work in various agency organizations that have different functions and are subject to different laws and regulations.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Not Applicable
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No

PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	There is no method for an individual to opt-out of the collection or use of their PII (Name and email address) because the information is required for a user to access the Lucid Govsuite service. The opt-out method of the collection of user phone number of mailing address would be for the user to not add their information to the documentation such as diagrams, charts, and text. This PII data is neither required nor specifically collected withing Lucid Govsuite.

PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	No changes to the data uses are anticipated. However, if there were significant changes to the system, a new PIA would be performed which would serve as notice to these individuals. Consent would be implied through the use of the tool. Additionally, Individual users of Lucid Govsuite are presented with the CDC standard System Use Notification (Warning Banner) at Log-In. The Notice reads: "Conditions of Use and Logon: You are accessing a US Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network., This information system is provided for US Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following:, You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system., Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose." Individuals are not contacted via name or email address as their consent is implied as a condition of their employment with CDC and their agreement to the CDC standard System Use Notification (Warning Banner) at Log-In. User phone numbers and mailing address documentation is only recorded at the discretion of the user for use in project specific documentation. There is no instances where individuals would be contacted about the Lucid system without their prior self-disclosure of their phone number or mailing address.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	If individuals believe that their information has been compromised or inappropriately used/obtained/disclosed, they can contact the Computer Security Incident Response Team (CSIRT) via email (CSIRT@cdc.gov), or by calling 1-866-655-2245. The CSIRT works with CDC Privacy Team to resolve PII incidents and mitigate the risks associated with the inadvertent loss or unapproved disclosure of personally identifiable information (PII).

PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	Lucid Govsuite System Administrators on a quarterly basis reviews the CDC configuration of the agency' s configuration of Lucid Govsuite to ensure the following: review account access; in the following areas: enabling, modifying, disabling and removing account access and to ensure that only identified and registered CDC assigned personnel have access to Lucid Govsuite.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: To provide a collaborative platform for creating diagrams and brainstorming using the individuals name/email listed in the system. The Lucid application gathers and track first name, last name, and email of the user of the application for follow up purposes. Administrators: Administrators create, manage, and monitor user accounts. Contractors: The Cloud Service Providers (CSP) non-direct contractors provide the hosted environment for Lucid Govsuite. The CSP has access to the system PII and provides maintenance support for the system. PII data is not viewable by Lucid Govsuite account holders.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users (i.e., those authorized to use Lucid Govsuite) and administrators that have completed CDC onboarding and personnel security processes, including security awareness and privacy training, are able to access the contents of documents that they create or are shared with them. CDC's use of Lucid Govsuite is leveraging the built-in groups for managing the different levels of access to a user is allowed upon the Lucid Govsuite system. The CDC defined User Groups within the Lucid Govsuite system are the following: Administrators and Standard Users which are required to obtain access authorization from the Lucid Govsuite system stewards before its granted via the Lucid Govsuite access control system.

PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	Roles within the Lucid Govsuite application are assigned based upon Role Based Access Controls (RBAC) and the least privilege model. The assignments correspond to the performance of their required duties which are defined to be either Users or Administrators. Enforcement of this access is implemented by a Role Based Access Control methodology which uses a least privileges model to determine access ability based on job roles. Lucid Govsuite system administrators with the appropriate permissions, who have signed Rules of Behavior and performed the required training are able to access the contents of documents for authorized purposes such as for troubleshooting. Users are only able to access documents that they have created or that have been shared with them specifically.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	All users are required to complete annual Information Security Training and Privacy Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users are provided training regarding the basic concepts of accessing services offered by the Lucid Govsuite cloud-based solution. Lucid Govsuite Administrators are required to complete training in Security Incident Response, Contingency Planning and Operations, and Role-Based training. This training is required to be completed when onboarding as a CDC employee and renewed annually.

PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The General Records Schedule (GSR) 5.5, item 10 (DAA-GRS-2016-0012-0001) and item 020 (DAA-GRS-2016-0012-0002) provide the specific retention schedules. GRS 5.5, item 10 Disposition Authority: DAA-GRS2016-00120001. Destroy when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use. GRS 5.5, item 20 Disposition Authority: DDAA-GRS2016-00120002. Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	ADMINISTRATIVE CONTROLS: PII is secured within the system through the use of administrative controls in the form of mandatory security awareness and privacy training for all users; role-based training for privileged users; personnel screening as required by CDC; completion of contractual agreements and Rules of Behavior; in accordance with applicable CDC policies. TECHNICAL CONTROLS: Technical controls applied to Lucid Govsuite include continuous network/system monitoring; compliant encryption of data in transit; firewalls; and authentication where applicable. PHYSICAL CONTROLS: Physical controls include Hosting within data centers which control and monitor physical access to the system components, including visitor control and auditing of access records; and, protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	1/28/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	2/3/2025
		SOP Days Open:	11

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/13/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 2/13/2025 All comments have been addressed, this PIA is ready for SAOP review and approval. PTA-5A response: Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is - Active Directory (AD) and Personal Identity Verification (PIV) card. PTA-8 response: Yes PTA-14 response: No PTA-20 response: Yes Per CDC Email (See Supporting Documentation) PTA-12A: Per the system owner, the correct response is “Session Cookies – Collect PII” Here is the documentation link Based on https://lucid.co/cookies?page=21#otnotice-section-3dc7d684-3be2-4114-aea7-95b47be0ac2a, they collect 1. email 2. username (could be first name, last name) but all of which would be federal employees or federal contractors as those are the personnels who will login to Lucid Govsuite. And for personnels who are not logging in, they generate an identifier to identifier users to place ads.	**Agency Privacy Analyst Days Open:**	10

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	2/20/2025
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Copy_of_Lucid_PIA_bl (12).rtf	249947	.rtf	2/6/2025 2:55 PM	0
RE Lucid -CDC7762606.msg	157696	.msg	2/13/2025 7:46 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 4	Data Feed Service, piafrmcdc	12/31/2024	How does phone number and mailing address provide access to access to Lucid Govsuite?	
PIA - 13	Data Feed Service, piafrmcdc	12/31/2024	What about phone numbers & mailing address? You only mention name & email address in you remarks.	
PIA - 14	Data Feed Service, piafrmcdc	12/31/2024	Although you don't anticipate any changes to the data, what happens when there is a change to the system itself? You collect email, phone number and mailing address. Do you not use these to contact the individuals? If so, please explain the process. If not, explain why not.	
PIA - 19	Data Feed Service, piafrmcdc	12/31/2024	Who within the CDC makes that determining factor? In other words, since Administrators and Standard Users have access to the PII, who grants them their rights and what is their procedure?	
PIA - 20	Data Feed Service, piafrmcdc	12/31/2024	Role Based Access Controls (RBAC) is better suited for PIA-19. What are the technical controls that limit a user's access to the type, amount, or categories of PII necessary to perform their job functions? Focus on system controls.	
PIA - 22	Data Feed Service, piafrmcdc	12/31/2024	What`s the frequency of this training?	
PIA - 22	Data Feed Service, piafrmcdc	1/23/2025	Is the frequency of the training daily,	

			weekly, monthly and/or annually?
PIA - 1	VILLAFUERTE, NESTOR	2/5/2025	Reviewer notes that PTA-8,14,&20 failed to sync. PIA-1 - Phone numbers and mailing address are selected but are not mentioned within the PTA.
PIA - 1	BLAND, CRYSTAL	2/6/2025	PTA-5A and PTA-5B: Please provide a response. PTA/12A: Should the response have been Session Cookies- Do Not Collect PII vs, Session Cookies- Collect PII. Please clarify and if PII is collected please explain in PTA-5 the PII collected and why the session cookies collect the PII.
PIA - 1	BLAND, CRYSTAL	2/6/2025	PTA-5A response: Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is - Active Directory (AD) and Personal Identity Verification (PIV) card. PTA-8 response: Yes PTA-14 response: No PTA-20 response: Yes
PIA - 1	BLAND, CRYSTAL	2/13/2025	Per CDC Email (See Supporting Documentation) PTA-12A: Per the system owner, the correct response is “Session Cookies – Collect PII” Here is the documentation link Based on https://lucid.co/cookies?page=21#otnotice-section-3dc7d684-3be2-4114-aea7-95b47be0ac2a, they collect 1. email 2. username (could be first name, last name) but all of which would be federal employees or federal contractors as those are the personnels who will login to Lucid Govsuite. And for personnels who are not logging in, they generate an identifier

to identifier users to place ads.

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	2/20/2025 3:01 PM	**History Log:**	View History Log